U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

April 8, 2020

BY ECF
The Honorable Lewis A. Kaplan
United States District Judge
Southern District of New York
500 Pearl Street, Room 2240
New York, New York 10007

Re: *United States* v. *Richard Liriano*, 19 Cr. 796 (LAK)

Dear Judge Kaplan:

The Government respectfully submits this letter in advance of the sentencing of the defendant, Richard Liriano ("Liriano" or the "defendant"), scheduled for April 15, 2020, and in response to Liriano's sentencing submission filed on March 31, 2020 ("Def. Let."). The defendant pled guilty, pursuant to a plea agreement, to a single-count computer intrusion scheme in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i). The plea agreement calculates the defendant's applicable United States Sentencing Guidelines ("Guidelines") range as 30 to 37 months' imprisonment (the "Stipulated Guidelines Range"). The United States Probation Office, in its revised Presentence Investigation Report dated March 12, 2020 (the "PSR") recommends a sentence of 30 months' imprisonment. For the reasons explained below, the Government submits that a sentence within Stipulated Guidelines Range is appropriate in this case and would be sufficient, but not greater than necessary, to achieve the legitimate purposes of sentencing.

I. Background

A. Offense Conduct

For about five years, Richard Liriano, an information technology employee at a New York-based hospital (the "Hospital") repeatedly, and opportunistically, spied on and hacked dozens of his female co-workers' work and personal e-mail and other storage accounts to search for sexually explicit images and videos. (PSR ¶ 8.) Liriano's coworkers trusted him to fix technical issues on their computers so that they could continue to serve patients and fulfill the Hospital's vital healthcare mission. Liriano repaid that trust by surreptitiously installing malicious software on his victims' computers, stealing log-in credentials for their personal e-mail accounts, and amassing a collection of their confidential documents and intimate files, for his own personal enjoyment. (PSR ¶¶ 10-13.) When caught, Liriano lied to the Hospital about the extent of his intrusions, wiped the evidence from his home computer, and sporadically continued to log into his victims' personal accounts. (PSR ¶¶ 15-17.)

Liriano's scheme began in 2013, about five years after he began working at the Hospital, and ran until he was caught in September 2018. (PSR ¶ 8.) It was time-consuming and methodical. The defendant's early intrusions were opportunistic. When called out to fix a technical problem in person, Liriano would use an unauthorized malicious program to secretly scan his victim's work computer for any user names and passwords used by his victim to log into their personal e-mail. (PSR ¶ 10.) As time went on, the defendant came up with a way to steal his victims' personal credentials without needing to physically attend to their computer during a service issue. (PSR ¶ 11.) Using the remote access available to him as an IT tech, Liriano secretly remotely installed a program commonly known as a keylogger on his co-workers' computers. (PSR ¶ 11.) The keylogger then secretly recorded and sent victim employees' keystrokes to Liriano, such as the usernames and passwords those employees entered to access their personal web-based email accounts, like Yahoo! or Gmail. (PSR ¶ 11.) Through the course of this conduct, Liriano stole usernames and passwords for at least approximately 70 email accounts belonging to the Hospital employees or persons associated with those employees (the "Compromised Personal Accounts"). (PSR ¶ 12.)

Liriano then used those stolen usernames and passwords to log in to his victims' Compromised Personal Accounts and obtain unauthorized access to their other non-work password-protected email, social media, photographs, videos and online social accounts. (PSR ¶ 13.) Among other things, Liriano conducted searches for sexually explicit photographs and videos in these personal accounts and their associated electronic storage. (PSR ¶ 13.) Many storage and email platforms store their users' files and data indefinitely, including media that could have been created when Liriano's victims were younger, and/or before they joined the Hospital. Liriano downloaded these highly private files onto his personal home computer. (PSR ¶ 13.) Liriano admitted to law enforcement following arrest that he chose his female victims based on "attractiveness," and that he used their personal files for his own sexual gratification. (PSR ¶ 19.)

Liriano used sophisticated technical means to commit the crime, including by remotely installing the keylogger and accessing his coworkers' personal folders and password-protected email accounts. (PSR ¶ 14.) The defendant engaged in this criminal conduct from his computer at the Hospital and from his personal computer at his home in the Bronx, among other means. (PSR ¶ 14.) He concealed evidence of his intrusions by deleting browsing history and other forensic evidence on his work computer, and using a Virtual Private Network to mask the source of his intrusions from his home in the Bronx. (PSR ¶ 15.) This meant that for years, Liriano's victims, working alongside him to fulfill the Hospital's patient-centered mission, had no idea that Liriano was secretly and repeatedly, accessing their work and personal storage, and gratifying himself on their most private files.

The defendant's scheme was first detected in late September 2018. (PSR ¶ 9.) The defendant logged into a victim's ("Victim-1") personal e-mail account on or about September 27 and 28, 2018, while remotely connected to the Hospital's network from his home. (PSR ¶ 9.) Despite taking precautions to make it appear to the victim's e-mail provider as if the victim herself was logging in from the Hospital (as she had done previously), the e-mail provider nonetheless reported a suspicious log-in to the victim, who in turn reported the associated log-in data to the Hospital. (PSR ¶ 9.) Forensic evidence tied the log-in to Liriano's home computer

and showed that Liriano conducted searches for photographs, and messages from this victim's fiancée. (PSR ¶ 9.) The defendant also e-mailed certain social media credential information out of Victim-1's account to a secondary e-mail account that Liriano maintained. (PSR ¶ 9.)

After being confronted by the Hospital, on or about October 10, 2018, the defendant signed a statement admitting to the September 27-28 intrusion only:

> I am employed by [the Hospital] as a Support Tech II. On September 27 - 28, 2018, I accessed [the Hospital's] employee's personal email and social media accounts, downloading pictures to my [Hospital] workstation and personal computer (the Incident). My access to, and downloading of, private employee information violated [the Hospital's] Code of Conduct and "Acceptable Use of Hospital Information Systems, Computers and Networks" policy. . . . (PSR ¶ 16.)

Although Liriano's statement only acknowledged intrusion into a single employee's personal email and social media accounts, a forensic analysis subsequently undertaken by the Hospital and the FBI revealed that the scope of Liriano's criminal conduct was far more extensive, and that Liriano had in fact had installed keyloggers on at least 44 workstations belonging to other employees. (PSR ¶ 17.) As noted above, Liriano also separately used a different malware program to collect his coworkers' personal email credentials before using the keylogger.

In or about October 2018, Liriano turned over his personal computer to the Hospital and stated that he deleted his coworkers' private files. (PSR ¶ 18.) An subsequent inspection indicated that Liriano wiped certain electronic data from his home computer, making it difficult to assess what he files he pilfered from what victims. Although Liriano was terminated, his criminal intrusions did not fully stop. He admitted to the FBI that in the Summer of 2019, he re-accessed personal password-protected accounts of two of his victims. (PSR ¶ 18.)

Liriano's crimes caused a variety of harms to the Hospital and the individual victims. Liriano's coworkers had to learn that their privacy—and the privacy of their significant others and anyone else whose corresponded with them—was repeatedly violated in an incredibly disturbing and voyeuristic way, causing obvious emotional damage. The Hospital confronted a massive privacy intrusion and security breach, learning that its own employee had for years been planting malware and unauthorized software onto its network, creating a generalized security risk to other intruders and hackers. As a result, the Hospital was required to engage in an extensive forensic examination, involving over 1,000 hours of work, to ensure the integrity of its systems, which serve critical functions, and contain sensitive health care data. Among others things, the Hospital had to identify and clean all of the computers affected by the malicious programs, and interview potentially affected employees. (PSR ¶ 20.) The Hospital incurred at least $351,850.25 in losses and remediation costs as a result of Liriano's conduct, which diverted the Hospital's time and resources away from its core healthcare function.

B. The Defendant's Arrest and Initial Charges

On November 14, 2019, the defendant was arrested on an Indictment that charged him with computer intrusion and aggravated identity theft, an offense that carried a two-year mandatory minimum sentence consecutive to the computer intrusion offense. (PSR ¶ 19.)

C. The Defendant's Plea

On December 20, 2019, the defendant pled guilty, pursuant to a plea agreement, to one count of computer intrusion, in violation of 18 U.S.C. 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(c)(4)(A)(i)(I) and (VI) and 2. (PSR ¶¶ 1-4.) In the Plea Agreement, the parties agreed that the defendant's base offense level is 6 under U.S.S.G. § 2B1.1(a)(2) G2.2(a)(1); a 12-level increase applied because the loss resulting from the offense was more than $250,000 but less than $550,000, pursuant to U.S.S.G. § 2B1.1(b)(1)(G); a 2-level increase was applied because the offense involved 10 or more victims, pursuant to U.S.S.G. § 2B1.1(b)(2)(A)(i); and a two-level increase applied because the defendant was convicted of an offense under 18 U.S.C. § 1030 and the offense involved an intent to obtain personal information, pursuant to U.S.S.G. § 2B1.1(b)(18)(A). (PSR ¶¶ 1-4.)

The parties also agreed that if the defendant clearly demonstrated acceptance of responsibility to the satisfaction of the Government, a two-level reduction would be warranted pursuant to U.S.S.G. § 3E1.1(a), and the Government would move at sentencing for an additional one-level reduction pursuant to U.S.S.G. § 3E1.1(b), resulting in an adjusted offense level of 19. (PSR ¶ 4.) As the defendant is in Criminal History Category is I, the Stipulated Guidelines Range is 30 to 37 months' imprisonment. (PSR ¶ 4.) The defendant's fine range is $10,000 to $100,000 pursuant to U.S.S.G. § 5E1.2. (PSR ¶ 4.)

D. Presentence Investigation Report

On March 12, 2020, the U.S. Probation Office ("Probation") issued the final PSR. Probation calculated the same Guidelines range as that set forth in the plea agreement and recommended a sentence of 30 months' imprisonment, at the low end of the Stipulated Guidelines range. (PSR at 17.) In support of its recommendation for a 30-month prison sentence, Probation noted that Liriano's "actions compromised the integrity of the Hospital for Special Surgery's computer systems and violated the trust of his employer and co-workers." (PSR at 18.)

E. Defendant's Sentencing Letter

In his March 11, 2020 submission, the defendant requested that the Court sentence him to a non-incarceratory sentence. (Def. Let. at 3.) The defendant's submission emphasized his lack of other criminal history, his strong family and friend support, and the fact that he did not appear to have distributed the stolen files to others or extorted his victims. (*Id.*)

II. Sentencing Legal Principles

Section 3553(a) of Title 18, United States Code, provides that the sentencing "court shall impose a sentence sufficient but not greater than necessary, to comply with the purposes" of sentencing outlined in Section 3553(a)(2) and then sets forth specific considerations,

including: the nature and circumstances of the offense and the history and characteristics of the defendant; the need for the sentence imposed to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, and to protect the public from further crimes of the defendant; the defendant's need for rehabilitation; the kinds of sentences available; the need to avoid unwarranted disparities in the sentences imposed on similarly situated defendants, and the sentencing range under the Guidelines. 18 U.S.C. § 3553(a).

Although no longer mandatory, the Guidelines continue to be an important sentencing factor. Indeed, because the Guidelines are "the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions," *Gall* v. *United States*, 552 U.S. 38, 46 (2007), the Supreme Court has instructed that the Guidelines are the "starting point and the initial benchmark" in sentencing proceedings. *Id.* at 49; *see also United States* v. *Rattoballi*, 452 F.3d 127, 133 (2d Cir. 2006) (the Guidelines '"cannot be called just 'another factor' in the statutory list, 18 U.S.C. § 3553(a), because they are the only integration of the multiple factors and, with important exceptions, their calculations were based upon the actual sentences of many judges.'") (quoting *United States* v. *Jiminez-Beltre*, 440 F.3d 514, 518 (1st Cir. 2006) (en banc)); *United States* v. *Crosby*, 397 F.3d 103, 113 (2d Cir. 2005) ("[I]t is important to bear in mind that *Booker/Fanfan* and Section 3553(a) do more than render the Guidelines a body of casual advice, to be consulted or overlooked at the whim of a sentencing judge."). After making the initial Guidelines calculation, a sentencing judge must then consider the other factors outlined in Title 18, United States Code, Section 3553(a), and "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing.

III. A Sentence of Incarceration Within the Stipulated Guidelines Range Would Be Just and Appropriate

The Government respectfully submits that a within the Stipulated Guidelines Range of 30 to 37 months' imprisonment would be a fair and appropriate sentence in this case. In particular, the nature and circumstances of the offense, the need for the sentence to reflect the seriousness of the offense and to provide just punishment, the need to promote respect for the law, and the need for adequate deterrence all justify such a sentence.

A. The Nature and Circumstances of the Offense

The defendant's scheme was extremely serious in its nature, scope, sophistication, duration, and impact. Abusing the access afforded to him as an IT professional, the defendant breached the integrity of a hospital network to satisfy his own prurient interests. He installed keyloggers and used other malicious software on multiple computers in a hospital that housed vital patient information. Those programs surreptitiously recorded the keystrokes of Liriano's coworkers and sent Liriano their credentials. Liriano then logged into their private email accounts to pilfer their personal files and media.

These electronic intrusions caused substantial harm. As the Honorable Judge Allison A. Nathan recently recognized in another case involving hacking for intimate files, "[b]reaking into

these spaces the way that Mr. Powell did, helping himself to private intimate imagery can in this day and age be just as serious, just as much an invasion as doing so through a bedroom window or breaking into someone's home." *United States v. Jonathan Powell*, 17 Cr. 340, Doc. No. 54, Mar. 1, 2018 Sentencing Tr. at 23. It is not difficult to imagine the indignity, angst, and embarrassment felt by the defendant's known victims when notified by the Hospital – their employer – about the nature of the intrusions. Liriano's conduct also carried a significant financial toll, requiring the Hospital to conduct an extensive forensic investigation to identify affected computers and employees, costing at least $351,850.25, and diverting the Hospital's time and resources from its core healthcare functions.

Liriano's offense was not a one-off "mistake" or momentary lapse of judgment. To the contrary, the conduct lasted approximately five years and involved hundreds, if not thousands, of individual criminal decisions. Liriano deliberately chose each of his approximately 70 victims. He searched for documents, tax records, and photos from folders on their work computers. He obtained and brought into the Hospital malicious spying programs. He waited for, and seized, opportunities to install those programs. He tracked data from those malicious programs, scanning for his victims' e-mail credentials to private, off-work, e-mail accounts. He chose when to log into his victims' personal accounts. He chose what to search for, what messages to read, and what files to download from those accounts. He chose when to go back for more. He came up with ways to conceal his tracks, like logging in through a virtual private network that would reduce the likelihood that the log-ins would be traced to his home computer.

Moreover, the defendant engaged in the charged scheme notwithstanding the fact that commercially-produced sexually explicit material was widely available for download on the Internet. Instead, the defendant chose to target specific known victims to satisfy his perverse desires. The violations of privacy he committed are extremely personal. The defendant's victims were not random strangers hacked from afar. They were people who *knew* and *trusted* the defendant to fix technical issues on their work computers, so that they could do the Hospital's critical work. They interacted with him on a regular basis, having no idea that he had hacked his way into their personal email accounts and was secretly accessing their correspondence, spying on their lives, and stealing and gratifying himself on their most intimate files. Such substantial, pervasive, and needless harm calls for a significant punishment.

The applicable Guidelines section, Section 2B1.1, appropriately focuses on the financial harm caused by the defendant's actions. The defendant, having made a conscious decision to abuse the authority placed in him by a major hospital – an institution houses troves of personal and confidential data – is rightly responsible for the many steps taken and associated costs incurred by in investigating the compromise, rooting out the intruder, and engaging in appropriate remediation. *See* U.S.S.G. § 2B1.1, Application Note 3(A)(v)(III) (defendants convicted of 18 U.S.C. § 1030 responsible for "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service," even where "such pecuniary harm was not reasonable foreseeable"); *see also United States* v. *Musacchio*, 590 F. App'x 359, 365 (5th Cir. 2014) ("Note 3(A)(v)(III) was designed to more fully account for

specific factors relevant to computer offenses") (internal quotations omitted, emphasis in original).

Insofar as financial loss largely drives the offense level under Section 2B1.1, however, the Guidelines do not directly address the more pernicious harm caused by the defendant's conduct, namely, his surreptitious, unwanted, and unauthorized intrusion into very sensitive and personal aspects of his victims' lives. That harm is difficult to quantify, but it is plainly extensive. The defendant deliberately and systematically hacked into the email and social media accounts of approximately 70 victims, invading their privacy and, in some cases, stealing their photographs and videos of their most intimate moments. He did so on a regular basis.

In sentencing a defendant on somewhat similar (but certainly not identical) offenses,[1] the Honorable Judge Paul A. Engelmayer eloquently described the inadequacy of the Guidelines as applied to such cybercrime privacy violations, the true harm of those violations, and the need for correspondingly significant punishment, including for the purpose of deterring others from committing similar crimes:

> [Y]our crimes are deeply troubling. The sentence I impose here needs to reflect the seriousness of your conduct. Significantly, here, the sentencing guidelines for your two offenses in my judgment are not nearly up to the task of capturing the harm you intended to do.
> * * * * *
> The guidelines as applied here do not assign any weight to the [non]monetary harm caused by your hacking and selling of celebrities' personal documents and photographs. They do not assign any weight to the emotional wallop to a person, whether celebrity or not, of knowing that her private intimate pictures are circulating among strangers.
> * * * * *
> At a time when much of the world has a presence on the Internet, at a time when so many people in this country and abroad keep sensitive material on line, whether personal data or confidential business information or work, at a time when remote hacking is regrettably an all-too-common topic in our news, it is vitally important that the law muscularly respond to the modern-day pirates like you who would plunder that material. The sentences in such cases of cybercrime need together to send a message that significant punishment awaits hackers who access accounts for purposes of theft and self-enrichment. The sentence imposed here has the potential to convey that message to those . . . who would follow your lead.

[1] The defendant in the case before Judge Engelmayer, Alonzo Knowles, hacked into the online accounts of celebrities and others, and later distributed certain stolen sexually explicit images and copyrighted materials for financial gain. In this case, the Government does not dispute the defendant's assertion that he did not distribute any of the materials that he stole, and agrees that his actions were not driven by any financial motive. However, unlike in the *Knowles* case, the conduct here is aggravated by the defendant's abuse of his position at the Hospital.

See United States v. *Alonzo Knowles*, 16 Cr. 005 (PAE), Doc. No. 49, Dec. 6, 2016 Sentencing Tr. at 45, 48, 49-50.

B. The Need to Afford Adequate Deterrence

One of the paramount factors that the Court must consider in imposing sentence under Section 3553(a) is the need for the sentence to "afford adequate deterrence to criminal conduct." 18 U.S.C. § 3553(a)(2)(B). There is a heightened need for specific deterrence in this case. The defendant was not deterred by the prospect of losing his job and facing criminal sanctions during the five years that he persistently victimized his female co-workers. If his last workplace intrusion in September 2018 had not been caught, it is clear that the defendant would have continued to hack and steal his victims' files through his position. In fact, the defendant's firing did not actually cause him to refrain from this misconduct; as he admitted, the defendant intruded into two of his victims' accounts months after he was fired.

Further, there is nothing to indicate that whatever perverse compulsions played a role in this conduct are being treated or addressed in any way by the defendant, and will not cause him to reoffend in the future. The defendant elected not to discuss this offense with Probation and he has (thus far) elected not to submit any personal statement to the Court with his sentencing submission. He has not yet expressed any genuine remorse. He has not demonstrated any understanding of the harm he caused. Given the long-running and seemingly pathological nature of this offense, the Government respectfully submits that a Guidelines sentence is necessary to truly impress upon Liriano the wrongfulness of his actions and deter him from future misconduct.

Because these types of hacking offenses are more cool and calculated than sudden crimes of passion or opportunity, they are also prime candidates for general deterrence. As Judge Nathan remarked in the *Powell* case, "[p]erhaps most importantly, given the extent of the harm and the pervasiveness of our modern online and electronic existence, the difficulty that law enforcement has in investigating these kinds of crimes, the difficulty of cracking them and finding the perpetrators and bringing them to justice, and also given the profile of someone like Mr. Powell who engages in this crime, general deterrence is of utmost importance." *United States* v. *Jonathan Powell*, 17 Cr. 340, Doc. Nso. 54, Mar. 1, 2018 Sentencing Tr. at 23-24.

In the modern professional workplace, sophisticated information technology specialists entrusted to maintain the integrity of workplace technology can abuse that access to devastating ends. A significant prison sentence—within the Guidelines range—is necessary to send a message that any such violation of trust will be met with serious punishment.

C. The History and Characteristics of the Defendant

The Government respectfully submits that there is nothing in the defendant's personal history and characteristics to meaningfully differentiate him from the heartland of cyber offenders. Although it is true that this five-year scheme represents the defendant's first criminal conviction, his criminal history is already factored into the Guidelines. His confession to law enforcement, while commendable, came only after he was arrested and facing overwhelming

forensic evidence and his own prior inculpatory statements. Further, unlike many other defendants before this Court, the defendant grew up with, and continues to enjoy, the support of his family and friends. His crime spanned his late twenties and early thirties and cannot be chalked up to some youthful indiscretion. There is nothing in the record—such as a psychiatric diagnosis or relevant history—that might explain his compulsion to commit these sexually-driven offenses or offer any reassurance that he would refrain from doing so in the future.

The defendant has submitted letters attesting to his positive personal qualities, and expressing surprise at his arrest and conviction. It is, of course, appropriate for the Court to take these letters into account in connection with sentencing. However, the Government asks that, in so doing, the Court consider the following three points. First, the attestations to Liriano's positive personal qualities do not distinguish him from other similarly situated white-collar defendants—individuals who, despite having opportunities and a network of people who love and support them, nonetheless choose to commit cyber offenses.

Second, the letter writers' attestations to Liriano's positive qualities have diminished value because the defendant has demonstrated a remarkable ability to deceive his co-workers about his criminal activities. While working with a team of other information technology professionals, including some of the letter-writers, Liriano managed to repeatedly and secretly install unauthorized software and steal his coworkers' personal files. Given that the defendant kept his family and friends in the dark about his criminal schemes, their attestations to his positive character do not bear significant weight.

Third, to the extent that Liriano or the letter writers suggest that the defendant's loss of professional standing as a result of his conviction warrants a lighter sentence (*see, e.g.*, Def. Let. at 3 ("As the result of his conviction, Liriano lost a job with a good salary he had held for 10 years."), this claim should be rejected. "It is impermissible for a court to impose a lighter sentence on white-collar defendants than on blue-collar defendants because it reasons that white-collar offenders suffer greater reputational harm or have more to lose by conviction." *United States* v. *Prosperi*, 686 F.3d 32, 47 (1st Cir. 2012) (citing U.S.S.G. § 5H1.2); *see also United States* v. *Musgrave*, 761 F.3d 602, 608 (6th Cir. 2014) ("In imposing a sentence of one day with credit for the day of processing, the district court relied heavily on the fact that Musgrave had already 'been punished extraordinarily' by four years of legal proceedings, legal fees, the likely loss of his CPA license, and felony convictions that would follow him for the rest of his life. '[N]one of these things are [his] sentence. Nor are they consequences of his sentence'; a diminished sentence based on these considerations does not reflect the seriousness of his offense or effect just punishment." (citation omitted)).

Finally, it bears noting that as a benefit of the plea agreement, the defendant faces no mandatory minimum sentence, despite being arrested on a charge carrying a two-year mandatory minimum prison term that would have run consecutively to the hacking count. The Government respectfully submits that this substantial break more than sufficiently accounts for whatever potentially mitigating circumstances can be gleaned from the defendant's background and personal characteristics.

D. Conclusion

For the reasons set forth above, the Government respectfully submits that a sentence of incarceration within the Stipulated Guidelines Range of 30 to 37 months is fair and appropriate in this case. The defendant should also be ordered to pay restitution in the amount of $351,850.25 to the Hospital.

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney

By: /S/
Vladislav Vainberg
Assistant United States Attorney
Tel.: (212) 637-1029

cc: Jennifer Willis, Esq.